LISTING OF CLAIMS (REPLACES ALL PREVIOUS VERSIONS):

1. (Currently Amended) A method of transmitting data securely over a computer network, comprising the steps of:

(1) establishing a communication path between a first computer and a second computer;

(2) encrypting and transmitting data records between the first computer and the second computer using an unreliable communication protocol, wherein each data record incorporates a nonce and encrypted text that has been encrypted using the nonce and a shared encryption key and without reference to a previously transmitted data record; and

(3) in the second computer, receiving and decrypting the data records transmitted in step (2) by, for each of the received data records, decrypting the incorporated encrypted text using the incorporated nonce in combination with ~~a previously~~ the shared encryption key and without reference to a previously received data record,

further comprising the step of, in the second computer, verifying for each received data record that the incorporated nonce has not previously been received in a previously transmitted data record.

2. (Original) The method of claim 1, further comprising the step of, prior to step (1), establishing a reliable communication path between the first computer and the second computer and exchanging security credentials over the reliable communication path.

3. (Currently Amended) The method of claim 2, wherein the step of exchanging security credentials comprises the step of exchanging the shared ~~an~~ encryption key that is used to encrypt the data records in step (2).

4. (Canceled)

5. (Previously Presented) The method of claim 1, wherein the nonce comprises a random

number.

6. (Cancelled) The method of claim 1, further comprising the step of, in the second computer, verifying for each received data record that the incorporated nonce has not previously been received in a previously transmitted data record.

7. (Currently Amended) A method of transmitting data securely over a computer network, comprising the steps of:

(1) establishing a communication path between a first computer and a second computer;

(2) encrypting and transmitting data records between the first computer and the second computer using an unreliable communication protocol, wherein each data record incorporates a nonce and encrypted text that has been encrypted using the nonce and a shared encryption key and without reference to a previously transmitted data record; and

(3) in the second computer, receiving and decrypting the data records transmitted in step (2) by, for each of the received data records, decrypting the incorporated encrypted text using the incorporated nonce in combination with the shared encryption key and without reference to a previously received data record,

wherein step (2) comprises the step of embedding an indicator in each of the encrypted data records indicating that the encrypted data records incorporate encrypted text that has been encrypted according to an encryption scheme that encrypts text without regard to any previously transmitted data records, and

wherein step (3) comprises the step of determining whether the indicator is present in each received record and, in response to determining that the indicator is not present, processing each such record differently than if the indicator is set.

8. (Original) The method of claim 1, wherein step (1) is performed using the Transmission Control Protocol, and wherein step (2) is performed using the User Datagram Protocol.

9. (Original) The method of claim 1, wherein step (2) is performed by a proxy server that encrypts data records received from another server.

10-15. (Cancelled)

16. (Currently Amended) A system for securely transmitting data using an unreliable protocol, comprising:

a first computer comprising a communication protocol client function operable in conjunction with an application program to transmit data records securely using an unreliable protocol; and

a second computer coupled to the first computer and comprising a communication protocol server function operable in conjunction with the communication protocol client function to receive data records securely using the unreliable communication protocol,

wherein, for each data record, the communication protocol client function encrypts text for the data record using a nonce and an encryption key and incorporates the respective encrypted text and nonce in the data record; ~~and~~

wherein the communication protocol server function decrypts the encrypted text in each of the data records using the respectively appended nonce and the encryption key; and

wherein the second computer comprises a record detector that determines whether an indicator has been set in each data record received from the first computer and, if the indicator has not been set, bypasses decryption in the server computer.

17. (Original) The system of claim 16, wherein the communication protocol client

function exchanges encryption credentials with the communication protocol server function using a reliable communication protocol.

18. (Original) The system of claim 17, wherein the unreliable communication protocol comprises the User Datagram Protocol, and wherein the reliable communication protocol comprises the Transmission Control Protocol.

19. (Original) The system of claim 16, wherein the communication protocol client function and the communication protocol server function are compatible with the SOCKS communication protocol.

20. (Original) The system of claim 16, wherein the communication protocol client function and the communication protocol server function are compatible with the SSL/TLS communication protocol.

21. (Previously Presented) The system of claim 16, wherein the second computer comprises a proxy server that forwards the decrypted text to a server computer.

22. (Cancelled) The system of claim 16, wherein the second computer comprises a record detector that determines whether an indicator has been set in each data record received from the first computer and, if the indicator has not been set, bypassing decryption in the server computer.

23. (Currently Amended) A method of transmitting data securely over a computer network, comprising:

establishing a communication path with a remote computer;

encrypting data records using a nonce and a shared encryption key such that each data record incorporates

the nonce, and

text that is encrypted such that the remote computer can decrypt the encrypted text

by using the incorporated nonce in combination with the shared encryption key ~~a previously shared encryption key~~ and without reference to a previously received data record; and

transmitting the encrypted data records to the remote computer using an unreliable communication protocol,

wherein encrypting the data records includes embedding an indicator in each of the data records indicating that the data record incorporates text encrypted according to an encryption scheme that encrypts text without regard to any previously transmitted data records, such that the remote computer can determine whether the indicator is present in each received data record and, in response to determining that the indicator is not present, process each such received data record differently than if the indicator is set.

24. (Previously Presented) The method of claim 23, further comprising establishing a reliable communication path to the remote computer and exchanging security credentials with the remote computer over the reliable communication path.

25. (Previously Presented) The method of claim 24, wherein the step of exchanging security credentials includes exchanging an encryption key that is used to encrypt the text.

26. (Previously Presented) The method of claim 23, wherein the nonce includes a random number.

27. (Cancelled) The method of claim 23, wherein encrypting the data records includes embedding an indicator in each of the data records indicating that the data record incorporates text encrypted according to an encryption scheme that encrypts text without regard to any previously transmitted data records, such that the remote computer can determine whether the indicator is present in each received data record and, in response to determining that the indicator

is not present, process each such received data record differently than if the indicator is set.

28. (Previously Presented) The method of claim 23, wherein

establishing the communication path with the remote computer is performed using the Transmission Control Protocol, and

encrypting the data records is performed using the User Datagram Protocol.

29. (Previously Presented) The method of claim 23, wherein encrypting the data records is performed by a proxy server that encrypts text received from another server.

30. (Currently Amended) A method of transmitting data securely over a computer network, comprising:

establishing a communication path with a remote computer;

receiving data records

transmitted from the remote computer using an unreliable communication protocol, and

encrypted using a nonce and a shared encryption key such that

each data record incorporates a nonce and

text that is encrypted without reference to a previously encrypted data record; ~~and~~

decrypting the received data records by using the nonce in combination with a previously shared encryption key to decrypt each received data record without reference to a previously received data record; and

verifying that the nonce has not previously been received in a previously received data record.

31. (Previously Presented) The method of claim 30, further comprising establishing a

reliable communication path with the remote computer and exchanging security credentials with the remote computer over the reliable communication path.

32. (Previously Presented) The method of claim 31, wherein exchanging security credentials includes exchanging the shared ~~an~~ encryption key that is used to encrypt the received data records.

33. (Previously Presented) The method of claim 30, wherein the nonce includes a random number.

34. (Cancelled) The method of claim 30 further comprising verifying that the nonce has not previously been received in a previously received data record.

35. (Currently Amended) A method of transmitting data securely over a computer network, comprising:

establishing a communication path with a remote computer;

receiving data records

transmitted from the remote computer using an unreliable communication protocol, and

encrypted using a nonce and a shared encryption key such that

each data record incorporates a nonce and

text that is encrypted without reference to a previously encrypted data record; and

decrypting the received data records by using the nonce in combination with the ~~a~~ ~~previously~~ shared encryption key to decrypt each received data record without reference to a previously received data record~~The method of claim 30~~,

wherein the received encrypted data records include an indicator indicating that the data

records incorporate text that has been encrypted according to an encryption scheme that encrypts records without regard to any previously transmitted data records, and

further comprising determining whether the indicator is present in each received data record and, in response to determining that the indicator is not present in a received data record, processing such received data record differently than if the indicator is set.

36. (Previously Presented) The method of claim 30, wherein

establishing a communication path with a remote computer is performed using the Transmission Control Protocol, and

received the encrypted data records is performed using the User Datagram Protocol.

37. (Previously Presented) The method of claim 30, wherein the received data records are received from a proxy server that encrypts data records the proxy server received from another server.

38-67. (Cancelled)